

Notice of Allowability

Application No.

10/037,153

Examiner

Calvin L. Hewitt II

Applicant(s)

LAM ET AL.

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 9-30-06.
2. ☒ The allowed claim(s) is/are 36-58.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 6-29-06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Status of Claims

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark McCarthy and Robert Lord on 29 September 2006.

3. The Application has been amended as follows-

Claims 1-35 have been canceled.

36. (New) A method for securing encryption keys in a key management system (KMS) comprising:

receiving data into the KMS, wherein the data comprises a key, a key name, and a key type, and wherein the data is received from a client over a network;
receiving at least one key encryption key (KEK) into the KMS, wherein the KEK is received from the client using a smart card interfacing over the network with the KMS, wherein the smart card stores the KEK;
encrypting the key, the key name, and the key type using the KEK to generate a secret token, wherein the encryption is performed by the KMS;
hashing the KEK to generate a hashed KEK;
generating a vector comprising the secret token and the hashed KEK, wherein the secret token comprises the encrypted key;
serializing the vector to generate a serialized file; and
storing the serialized file in KMS memory.

37. (New) The method of claim 36, further comprising:
storing the key, the key name, and the key type in a 3-tuple prior to encrypting
the key, the key name, and the key type.
38. (New) The method of claim 37, further comprising:
encoding the key after storing the key in the 3-tuple.
39. (New) The method of claim 36, further comprising:
tagging the secret token to associate it with an application.
40. (New) The method of claim 36, wherein encrypting the key, the key name, and the
key type comprises:
using a symmetric algorithm.
41. (New) The method of claim 36, wherein encrypting the key, the key name, and the
key type comprises:
using an asymmetric algorithm.
42. (New) The method of claim 36, wherein receiving data into the KMS comprises:
using a graphical user interface.
43. (New) The method of claim 42, wherein the graphical user interface is integrated into
a web browser.
44. (New) The method of claim 36, wherein the serialized file persists beyond the time
the KMS is active and provides secure storage of the key and the KEK.
45. (New) A system for securing encryption keys comprising:
a key management system storage; and
a key management system (KMS) configured to:

- receive data into the KMS, wherein the data comprises a key, a key name, and a key type, and wherein the data is received from a client over a network;
 - receive at least one key encryption key (KEK) into the KMS, wherein the KEK is received from the client using a smart card interfacing over the network with the KMS, wherein the smart card provides the KEK;
 - encrypt the key, the key name, and the key type using the KEK to generate a secret token, wherein the encryption is performed by the KMS;
 - hash the KEK to generate a hashed KEK;
 - generate a vector comprising the secret token and the hashed KEK, wherein the secret token comprises the encrypted key;
 - serialize the vector to generate a serialized file; and
 - store the serialized file in KMS memory.
- 46.(New) The system of claim 45, wherein the KMS is further configured to store the key, the key name, and the key type in an 3-tuple prior to encrypting the key, the key name, and the key type.
- 47.(New) The system of claim 46, wherein the KMS is further configure to:
 encode the key after storing the key in the 3-tuple.
- 48.(New) The system of claim 45, wherein the KMS is further configured to:
 tag the secret token to associate it with an application.
- 49.(New) The system of claim 45, further comprising:
 a graphical user interface.
- 50.(New) The system of claim 49, wherein the graphical user interface is integrated into a web browser.

- 51.(New) The system of claim 45, wherein the serialized file persists beyond the time the KMS is active and provides secure storage of the key and the KEK.
- 52.(New) A computer readable medium storing instructions for execution on a key management system (KMS) processor, which when executed by the KMS processor cause the KMS processor to perform the steps of:
- receiving data into the KMS, wherein the data comprises a key, a key name, and a key type, and wherein the data is received from a client over a network;
 - receiving at least one key encryption key (KEK) into the KMS, wherein the KEK is received from the client using a smart card interfacing over the network with the KMS, wherein the smart card stores the KEK;
 - encrypting the key, the key name, and the key type using the KEK to generate a secret token, wherein the encryption is performed by the KMS;
 - hashing the KEK to generate a hashed KEK;
 - generating a vector comprising the secret token and the hashed KEK, wherein the secret token comprises the encrypted key;
 - serializing the vector to generate a serialized file; and
 - storing the serialized file in KMS memory.
- 53.(New) The computer readable medium of claim 52, wherein the instructions further comprise instructions for:
- storing the key, the key name, and the key type in a 3-tuple prior to encrypting the key, the key name, and the key type.
- 54.(New) The computer readable medium of claim 53, wherein the instructions further comprise instructions for encoding the key after storing the key in the 3-tuple.
- 55.(New) The computer readable medium of claim 52, wherein the instructions further comprise instructions for tagging the secret token to associate it with an application.

- 56.(New) The computer readable medium of claim 52, wherein the instructions further comprise instructions for using a symmetric algorithm.
- 57.(New) The computer readable medium of claim 52, wherein the instructions further comprise instructions for encrypting the key, the key name, and the key type using an asymmetric algorithm.
- 58.(New) The computer readable medium of claim 52, wherein the serialized file persists beyond the time the KMS is active and provides secure storage of the key and the KEK.

Reasons for Allowance

4. The present invention is directed to securing encryption keys.

Key security is old and well known. For example, Ginter et al. (US 5,892,900) teach maintaining cryptographic data within a tamper proof storage device ('900, figure 6). Auerbach et al. (US 5,673,316) disclose a Bill of Materials database comprising fields ('316, figure 3). One entry in the database is an encryption key denoted in a field as "ENCRYPTED PEK 3". This information conveys to one of ordinary skill the name of the key "ENCRYPTED PEK 3" and the type "PEK 3" (i.e. part encryption key of part 3). In the next column, the BOM provides a field containing the signature of the key or "value". Auerbach et al. also teach digitally signing and storing the BOM ('316, column 5, lines 19-44). To one of ordinary skill generating a digital signature through encryption is old and

well known (Applied Cryptography, Schneier, page 37). The closest prior art of Linehan et al. (US 5,495,533) teaches a database that stores a key, key name, key type in a database, wherein each entry in the database is encrypted ('533, figure 8; column 7, lines 39-45; column 8, lines 57-65). The present invention, however, recites a key management system receiving a key, key type, and key name from a client, a key encryption key from the client wherein the key encryption key is stored on a smart card and generating a secret token by encrypting the key, key name and key type. Auerbach et al. and Linehan et al. teach away from this aspect of Applicant's claims because in Auerbach et al. the system generates the keys ('316, column/line 4/65-5/13) while in the Linehan et al. system a secret token is not generated as a key, key name, and key type are not entered along with an encryption key ('533, column 8, lines 37-45). Therefore, as this feature is not taught by the prior art singly or in combination, it distinguishes the present claims from the prior art.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:
 - Saito et al. teach a ciphering key system

- M2 Presswire, Dec 6, 1996, "SCHLUMBERGER: Schlumbereger launches industry's most secure smart card"
- "Applied Cryptography", Second Edition, Schneier, pg 37

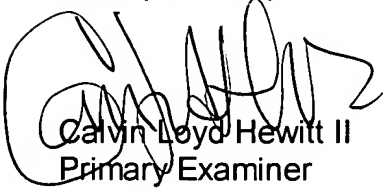
5. Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Fischer, can be reached at (571) 272-6779.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see [<http://pair-direct.uspto.gov/>](http://pair-direct.uspto.gov/). Should you have questions on access to the

Private PAIR system, contact the Electronic Business Center (EBC) at **866-217-9197 (toll-free)**.



Calvin Lloyd Hewitt II
Primary Examiner

October 2, 2006